

CLAIMS

What is claimed is:

- Sub A1
1. A system for establishing a secure execution environment for a software process executed by a program operating on a computer, comprising:
 2. a software process operating on a computer, said software process including a plurality of attributes;
 3. an operating system kernel in communication with said software process and in communication with an executable file to be accessed by said software process; and
 4. a system call trap associated with said operating system kernel, said system call trap configured to assign a selected plurality of said attributes to said software process, said selected plurality of attributes stored in association with said executable file.
 5. The system of claim 1, wherein said system call trap further comprises:
 6. a process attribute extension; and
 7. an access token extension associated with said process attribute extension, said access token extension including said selected plurality of attributes.
 8. The system of claim 1, wherein said selected plurality of attributes are contained in a database associated with said executable file.
 9. The system of claim 1, wherein said selected plurality of attributes are chosen from the group consisting of user ID, group IDs and privileges.

1 5. The system of claim 1, wherein said execution environment isolates
2 said software process from any other software process operating on said computer.

1 6. The system of claim 1, wherein said software process is a web server
2 process.

1 7. The system of claim 1, wherein said software process is a file transfer
2 process.

1 8. The system of claim 1, wherein said software process is a mail server
2 process.

1 9. The system of claim 1, wherein said selected plurality of attributes are
2 associated to said software process upon execution of said software process.

1 10. The system of claim 1, wherein said selected plurality of attributes
2 replaces any existing attributes associated with said software process.

1 11. A method for establishing a secure execution environment for a
2 software process executed by a program operating on a computer, the method
3 comprising the steps of:

4 operating a software process on a computer, said software process including a
5 plurality of attributes;

6 executing an operating system kernel in communication with said software
7 process, said operating system kernel in communication with an executable file to be
8 accessed by said software process; and

9 assigning a selected plurality of said attributes to said software process, said
10 selected plurality of attributes stored in association with said executable file.

1 12. The method of claim 11, further comprising the steps of:

2 executing a process attribute extension; and

3 executing an access token extension associated with said process attribute
4 extension, said access token extension including said selected plurality of attributes.

1 13. The method of claim 11, wherein said selected plurality of attributes
2 are contained in a database associated with said executable file.

1 14. The method of claim 11, wherein said selected plurality of attributes
2 are chosen from the group consisting of user ID, group IDs and privileges.

1 15. The method of claim 11, wherein said execution environment isolates
2 said software process from any other software process operating on said computer.

1 16. The method of claim 11, wherein said software process is a web server
2 process.

1 17. The method of claim 11, wherein said software process is a file transfer
2 process.

1 18. The method of claim 11, wherein said software process is a mail server
2 process.

1 19. The method of claim 11, wherein said selected plurality of attributes
2 are associated to said software process upon execution of said software process.

1 20. The method of claim 11, wherein said selected plurality of attributes
2 replaces any existing attributes associated with said software process.

1 21. A computer readable medium having a program for establishing a
2 secure execution environment for a software process executed by a program operating
3 on a computer, the program including logic for performing the steps of:
4 operating a software process on a computer, said software process including a
5 plurality of attributes;
6 executing an operating system kernel in communication with said software
7 process, said operating system kernel in communication with an executable file to be
8 accessed by said software process; and
9 assigning a selected plurality of said attributes to said software process, said
10 selected plurality of attributes stored in association with said executable file..

1 22. The program of claim 21, further comprising logic for performing the
2 steps of:
3 executing a process attribute extension; and
4 executing an access token extension associated with said process attribute
5 extension, said access token extension including said selected plurality of attributes.

1 23. The program of claim 21, wherein said selected plurality of attributes
2 are contained in a database associated with said executable file.

1 24. The program of claim 21, wherein said selected plurality of attributes
2 are chosen from the group consisting of user ID, group IDs and privileges.

1 25. The program of claim 21, wherein said execution environment isolates
2 said software process from any other software process operating on said computer.

1 26. The program of claim 21, wherein said software process is a web
2 server process.

1 27. The program of claim 21, wherein said software process is a file
2 transfer process.

1 28. The program of claim 21, wherein said software process is a mail
2 server process.

1 29. The program of claim 21, wherein said selected plurality of attributes
2 are associated to said software process upon execution of said software process.

1 30. The program of claim 21, wherein said selected plurality of attributes
2 replaces any existing attributes associated with said software process.

ADD AZ